Configureer een tijdgebaseerde toegangscontroleregel op FDM met rest-API

Inhoud

Inleiding

Dit document beschrijft hoe u een tijdgebaseerde toegangscontroleregel kunt configureren en valideren met Rest API in de FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defense (FTD)
- Firepower Device Management (FDM)
- Kennis van representatieve Overdracht van de Toepassingsprogrammeerinterface van de Staat (REST API)
- Toegangscontrolelijst (ACL)

Gebruikte componenten

De informatie in dit document is gebaseerd op FTD versie 7.1.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

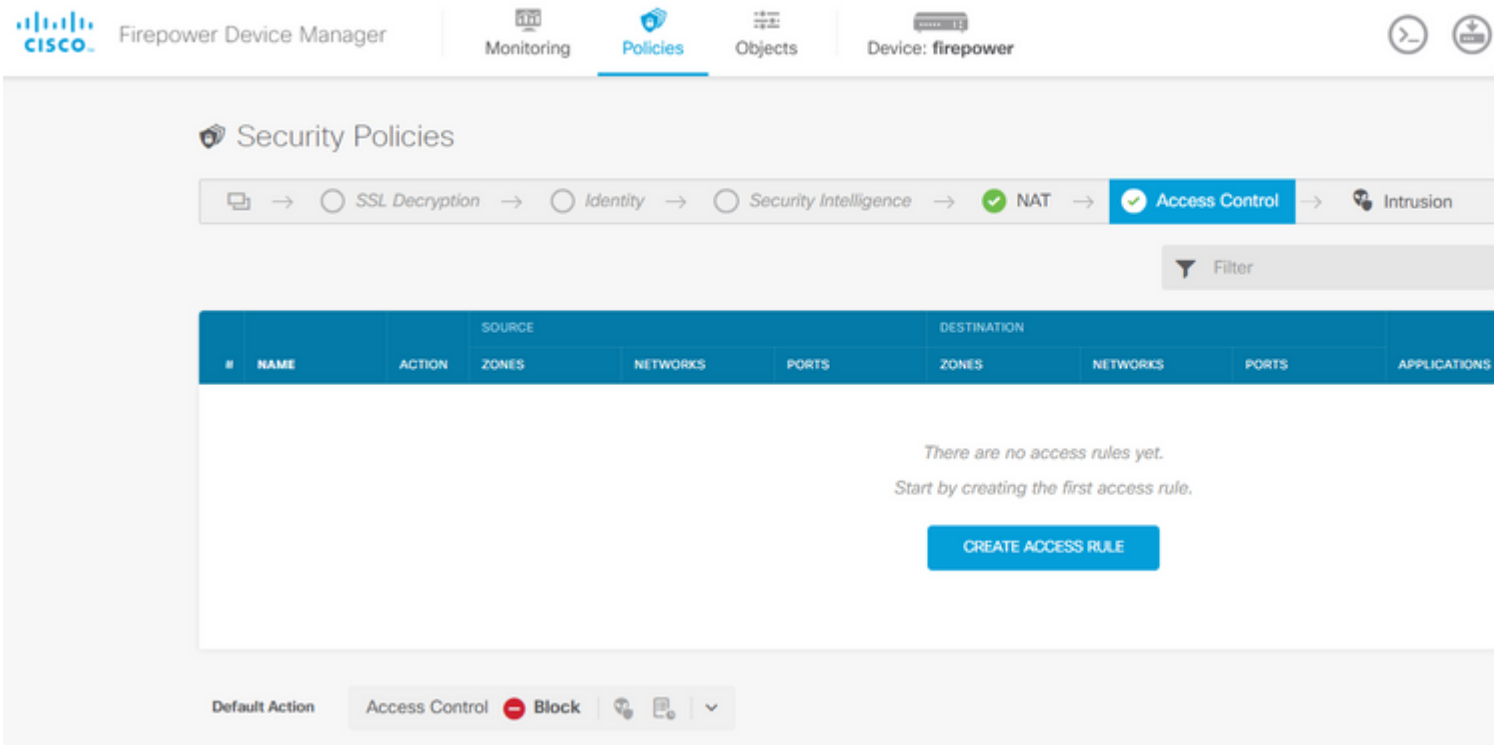
Achtergrondinformatie

FTD API versie 6.6.0 en hoger ondersteunen toegangscontroleregels die beperkt zijn op basis van tijd.

Met behulp van de FTD API kunt u tijdbereikobjecten maken, die eenmalige of terugkerende tijdbereiken specificeren, en deze objecten toepassen op toegangscontroleregels. Met behulp van tijdbereiken kunt u een toegangscontroleregel toepassen op verkeer tijdens bepaalde tijden van de dag of voor bepaalde periodes, om flexibiliteit te bieden aan netwerkgebruik. U kunt FDM niet gebruiken om tijdbereiken te maken of toe te passen, noch toont FDM u of een toegangscontroleregel een tijdbereik heeft toegepast op het.

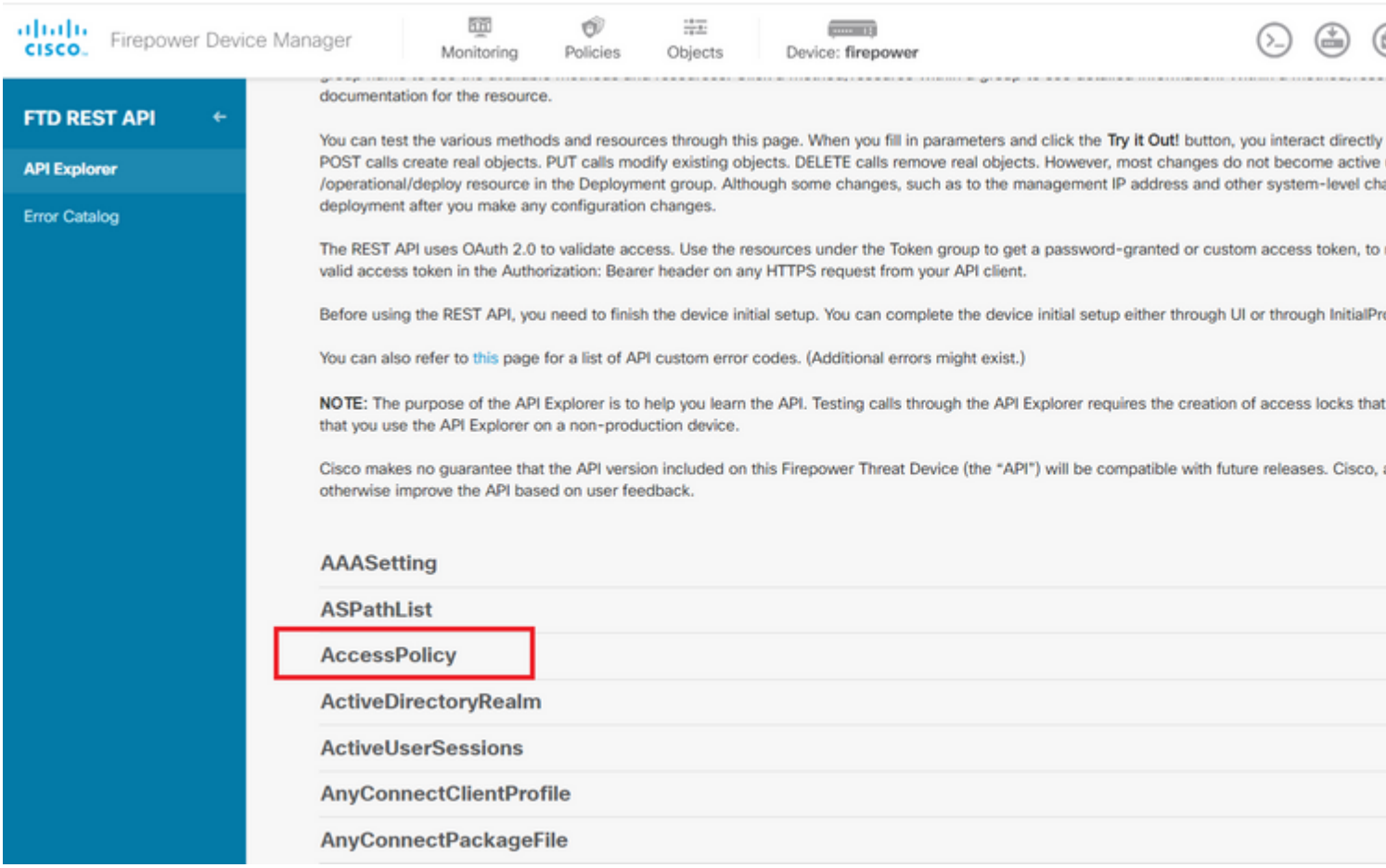
Configureren

Stap 1. Klik op de geavanceerde opties (het menu Kebab) om de FDM API verkenner te openen.



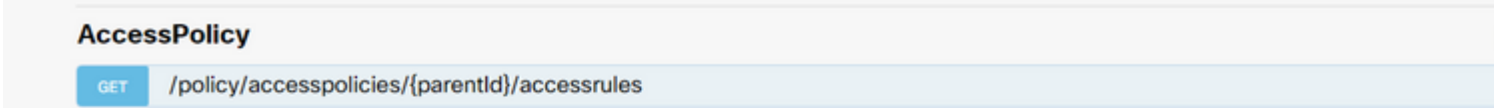
Afbeelding 1. FDM web gebruikersinterface.

Stap 2. Kies de categorie **AccessPolicy** om de verschillende API-oproepen weer te geven.



Afbeelding 2. API Explorer-webgebruikersinterface.

Stap 3. Draai de **GET** bellen om de Access Policy ID te verkrijgen.



formaat voorbeeld om de op tijd gebaseerde ACL te maken die verkeer van binnenuit naar de buitenzone toestaat.

Zorg ervoor dat u de juiste tijdbereik object-ID gebruikt.

<#root>

```
{
  "name": "test_time_range_2",
  "sourceZones": [
    {
          "name": "inside_zone",
          "id": "90c377e0-b3e5-11e5-8db8-651556da7898",
          "type": "securityzone"
    }
  ],
  "destinationZones": [
    {
      "name": "outside_zone",
      "id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
      "type": "securityzone"
    }
  ],
  "ruleAction": "PERMIT",
  "eventLogAction": "
```

LOG_FLOW_END

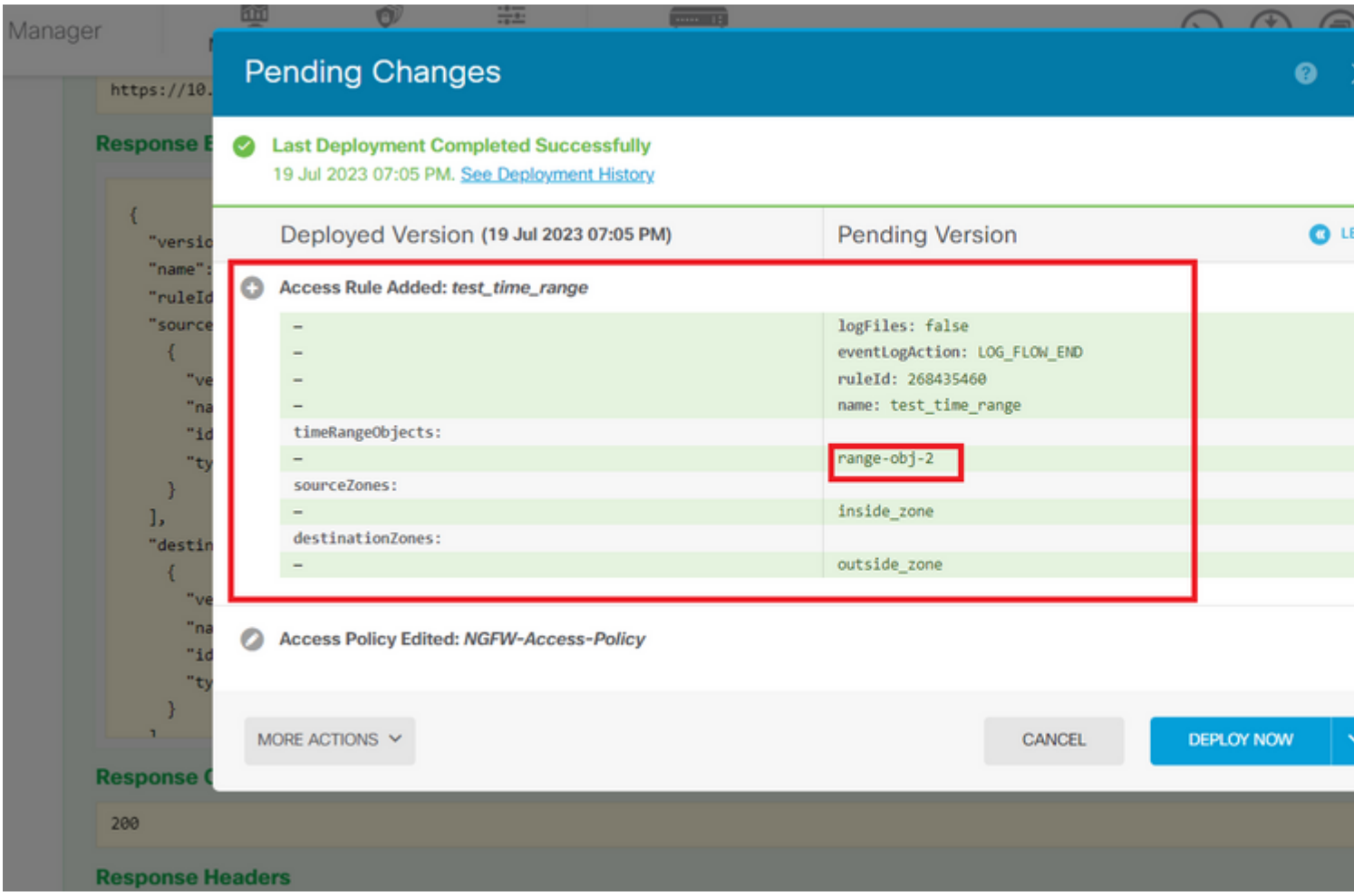
```
",
  "timeRangeObjects": [
    {
    "id": "
```

718e6b5c-2697-11ee-a5a7-57e37203b186

```
",
    "type": "timerangeobject",
    "name": "Time-test2"
    }
  ],
  "type": "accessrule"
}
```

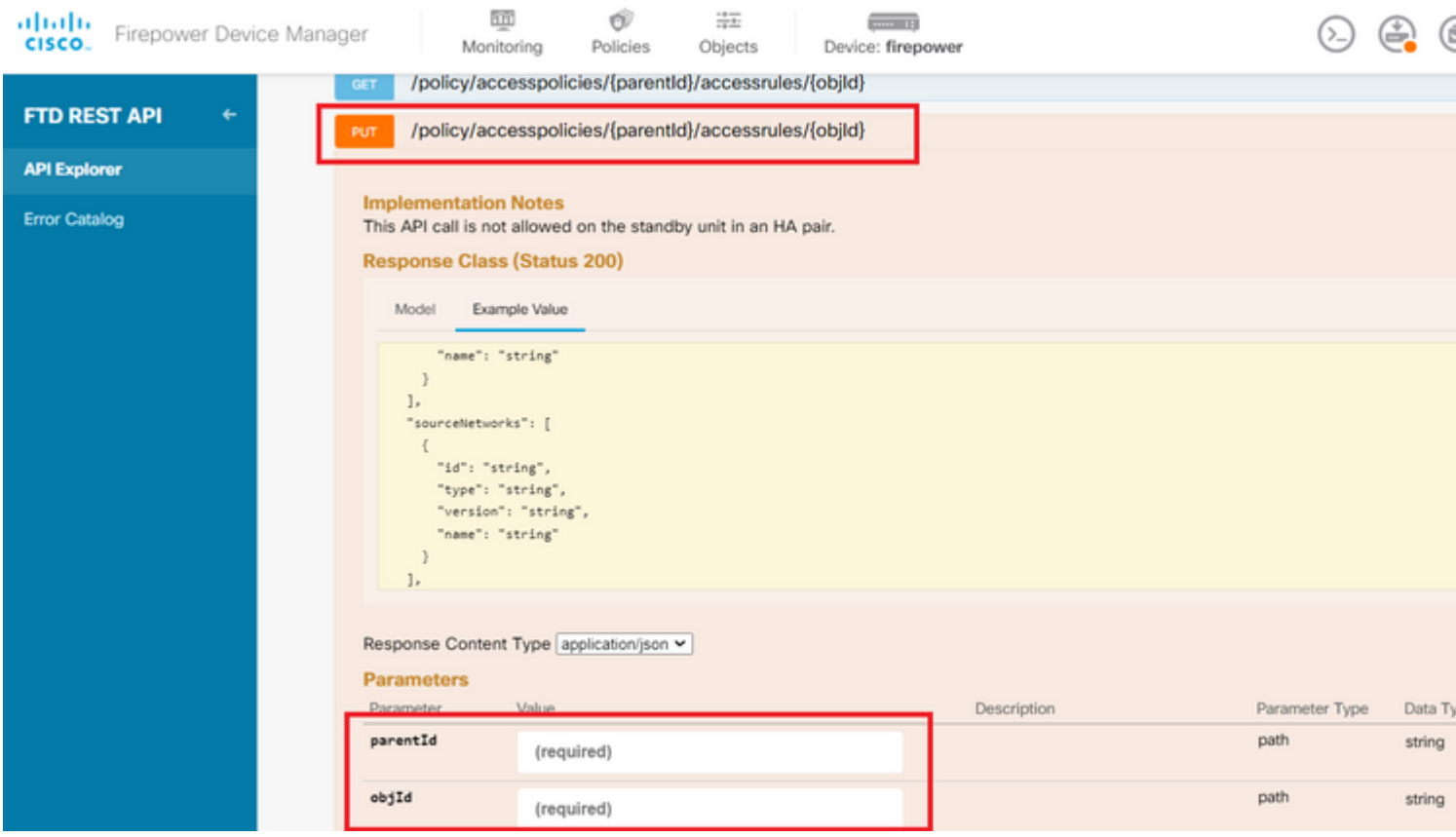
> **Opmerking:** eventLogAction moet **LOG_FlOW_END** om de gebeurtenis aan het eind van de stroom te registreren, geeft het anders een fout.

Stap 12. Stel de veranderingen op om nieuwe op tijd-gebaseerde ACL toe te passen. De wachtende melding Wijzigingen moet het in Stap 10 gebruikte tijdbereikobject weergeven.



Afbeelding 12. FDM In afwachting van het venster van Veranderingen toont de nieuwe regel.

Stap 13 (optioneel). Als u ACL wilt bewerken, kunt u de PUT de tijdbereik-ID bellen en bewerken.



Afbeelding 13. PUT call voor toegangsbeleid.

Vind hier de JSON Deze tijdbereik-ID's kunnen worden verzameld met behulp van de**GET** bellen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.